NIST Special Publication 800-29

A COMPARISON OF THE SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES IN FIPS 140-1 AND FIPS 140-2

Ray Snouffer
Annabelle Lee
Arch Oldehoeft

Security Technology Group
Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

June, 2001

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration

National Institute of Standards and Technology
Karen H. Brown, Acting Director

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-06-2001		xx-xx-2001 to xx-xx-2001

4. TITLE AND SUBTITLE
A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2 (NIST Special Publication 800-29)
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Snouffer, Ray ;
Lee, Annabelle ;
Oldenhoeft, Arch ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
National Institute of Standards and Technology
Gaithersburg, MD20899-8930

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, non-repudiation and identification and authentication. Adequate testing and validation of the cryptographic module against established standards is essential for security assurance. Both Federal agencies and the public benefit from the use of tested and validated products. Without adequate testing, weaknesses such as poor design, weak algorithms, or incorrect implementation of the cryptographic module, can result in insecure products.

15. SUBJECT TERMS
IATAC Collection; cryptography; cryptographic module; PKI; DES

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	30	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	6/1/2001	Report 6/1/2001

4. TITLE AND SUBTITLE
A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2 (NIST Special Publication 800-29)

5. FUNDING NUMBERS

6. AUTHOR(S)
Ray Snouffer, Annabelle Lee and Arch Oldenhoeft

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, non-repudiation and identification and authentication. Adequate testing and validation of the cryptographic module against established standards is essential for security assurance. Both Federal agencies and the public benefit from the use of tested and validated products. Without adequate testing, weaknesses such as poor design, weak algorithms, or incorrect implementation of the cryptographic module, can result in insecure products.

14. SUBJECT TERMS
IATAC Collection, cryptography, cryptographic module, PKI, DES

15. NUMBER OF PAGES
29

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

TABLE OF CONTENTS

1. THE CRYPTOGRAPHIC MODULE VALIDATION PROGRAM AND FIPS 140-2

Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, non-repudiation and identification and authentication. Adequate testing and validation of the cryptographic module against established standards is essential for security assurance. Both Federal agencies and the public benefit from the use of tested and validated products. Without adequate testing, weaknesses such as poor design, weak algorithms, or incorrect implementation of the cryptographic module, can result in insecure products.

On July 17, 1995, NIST established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-1 *Security Requirements for Cryptographic Modules,* and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-1 are accepted by the Federal agencies of both countries for the protection of sensitive information. Vendors of cryptographic modules use independent, accredited testing laboratories to test their modules. NIST's Computer Security Division and CSE jointly serve as the validation authorities for the program, validating the test results. Currently, there are several National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories that perform FIPS 140-1 compliance testing. These labs are listed at the web site: http://csrc.nist.gov/cryptval. As of January 2001 over 150 cryptographic modules from more than forty separate vendors have been validated through the program. The number of validated modules has nearly doubled each year of the program's existence.

The underlying philosophy of the CMVP is that the user community needs strong independently tested and commercially available cryptographic products. The CMVP must also work with the commercial sector and the cryptographic community to achieve security, interoperability and assurance. Directly associated with this philosophy is the goal of the CMVP to promote the use of validated products and provide Federal agencies with a security metric to use in procuring cryptographic modules. The testing performed by accredited laboratories provides this metric. Federal agencies, industry, and the public can choose products from the CMVP Validated Modules List and have confidence that the products meet the claimed level of security. The program validates a wide variety of modules including general encryption products, secure radios, Virtual Private Network (VPN) devices, Internet browsers, cryptographic tokens and modules that support Public Key Infrastructure (PKI). Currently, validation services are provided for FIPS 140-1 & 2, the Data Encryption Standard (DES and Triple DES), the Digital Signature Standard, the Secure Hash Standard, and the Skipjack Algorithm.

The CMVP offers a documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1&2 and other cryptographic standards. NIST developed the standard and an associated metric (the Derived Test Requirements for FIPS 140-1) to ensure repeatability of tests and equivalency in results across the testing laboratories. The five commercial laboratories provide vendors of cryptographic modules a choice of testing facilities and promotes healthy competition. (Note, there is no limit to the number of testing laboratories, and additional testing laboratories may be added to the program.)

A government and industry working group composed of both users and vendors developed FIPS 140-1. The working group identified eleven areas of security requirements with four increasing levels of security for cryptographic modules. The security levels allow for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and health data), and

a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Each security level offers an increase in security over the preceding level. These four security levels allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments. This structure also allows great flexibility when specifying or identifying users needs. Modules may meet different levels in the security requirements areas (e.g., a module meets level 2 overall, level 3 physical security with additional level 4 requirements). The Validated Modules list now contains modules representing all four security levels.

FIPS 140-1&2 define a framework and methodology for NIST's current and future cryptographic standards. The standard provides users with:

- a specification of security features that are required at each of four security levels;
- flexibility in choosing security requirements;
- a guide to ensuring the cryptographic modules incorporate necessary security features; and
- the assurance that the modules are compliant with cryptography based standards.

The Secretary of Commerce has made FIPS 140-1 mandatory and binding for U.S. Federal agencies and organizations. The standard is specifically applicable when a Federal agency determines that cryptography is necessary for protecting sensitive information. The standard is used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them. FIPS 140-1 is applicable if the module is incorporated in a product, application or functions as a standalone device.

From the beginning, the CMVP has been dynamic with a constant reexamination of the underlying standard, test methodology, reporting structure, and associated documentation. In addition, questions from the vendor and user communities have provided valuable input and an implementation perspective. NIST and CSE have continually kept pace with new security methods, changes in technology, and required interpretations of the standard by issuing official *Implementation Guidance and Policy* for FIPS 140-1 and associated *Derived Test Requirements* (DTR). The *Implementation Guidance* covers program policy, technical questions, and general guidance needed for module validation.

In addition to constant reexamination, the standard is officially reexamined and reaffirmed every five years. In the fall of 1998, FIPS 140-1 entered a regularly scheduled 5-year review to consider new and/or revised requirements needed to meet technological and economic change. A request for comments on FIPS 140-1 was published on October 23, 1998 in the Federal Register. The official comment period for the request closed January 21, 1999. A revised draft standard was produced based on the public comments received, previously issued implementation guidance and a "line by line" review by the NIST, CSE, and testing laboratory staff. A second request for comments on the resulting FIPS 140-2 draft was published on November 17, 1999 in the Federal Register with a closing date of February 15, 2000. In December 2000, the FIPS 140-1 update to FIPS 140-2 was completed. The implementation schedule for FIPS 140-2 begins with the approval date or date of signature. The effective date is six months after the approval date and marks the beginning of a six month transition period. This transition period enables agencies to develop acquisition plans for procuring FIPS 140-2 compliant modules. At the end of the transition period, modules will no longer be tested against FIPS 140-1. (Note: all FIPS 140-1 testing labs will become FIPS 140-2 testing labs.) However, FIPS 140-1 validated modules may continue to be procured. This paper gives an overview of the substantive differences between FIPS 140-1 and FIPS 140-2.

Section 2 of this document provides a summary analysis of the changes between FIPS 140-1 and 140-2. Section 3 of this document includes the specific requirements documented in FIPS 140-2 and the previous versions specified in FIPS 140-1. The FIPS 140-2 requirements are displayed in a box for easy reference.

2. SUMMARY OF DIFFERENCES BETWEEN FIPS 140-1 AND FIPS 140-2

FIPS 140-1 is one of NIST's most successful standards and forms the very foundation of the CMVP. FIPS 140-1 is widely recognized as the "defacto" standard for cryptographic modules and is referenced and/or used in its entirety by numerous standards bodies and international testing organizations. Therefore, great care was given to the update process beginning with a complete "line by line" review and examination of the standard and all *Implementation Guidance* issued during FIPS 140-1's initial five years. The underlying question asked by the authors of FIPS 140-2 was "how does one improve a successful and proven standard?" The answer was simple – include lessons learned from questions and comments, reflect changes in technology, and strengthen the standard, but do not change the focus or emphasis. The authors also took the opportunity to improve the format of the standard by minimally restructuring the content (see the table below), standardizing the language and terminology to add clarity and consistency, removing redundant and extraneous information to make the standard more concise, and revising or removing vague requirements. Looking to the future, the authors added a section detailing new types of attacks on cryptographic modules that currently do not have specific testing available. The end result is a stronger, more concise, and readable standard that still embodies the spirit of the original standard.

Tables of Content	
FIPS 140-1	*FIPS 140-2*
1. Overview	1. Overview
2. Glossary of Terms and Acronyms	2. Glossary of Terms and Acronyms*
3. Functional Security Requirements	3. Functional Security Requirements
4. Security Requirements	4. Security Requirements
4.1 Cryptographic Modules	4.1 Cryptographic Module Specification*
4.2 Cryptographic Module Interfaces	4.2 Cryptographic Module Ports and Interfaces
4.3 Roles and Services	4.3 Roles, Services, and Authentication*
4.4 Finite State Machine Model	4.4 Finite State Model
4.5 Physical Security	4.5 Physical Security*
4.6 Software Security	4.6 Operational Environment*
4.7 Operating System Security	4.7 Cryptographic Key Management
4.8 Cryptographic Key Management	4.8 EMI/EMC
4.9 Cryptographic Algorithms	4.9 Self-Tests*
4.10 EMI/EMC	4.10 Design Assurance*
4.11 Self-Tests	4.11 Mitigation of Other Attacks*
Appendixes	*Appendixes*
A: Summary of Documentation Requirements	A: Summary of Documentation Requirements
B: Recommended Software Development Practices	B: Recommended Software Development Practices*
C: Selected References	C: Cryptographic Module Security Policy*
	D: Selected Bibliography*

* Section added or significantly revised.

The following provides a brief discussion of each of the requirements areas and summary of the major changes.

2.1. Security Requirements

This section summarizes the changes from FIPS 140-1 to FIPS 140-2.

2.1.1. Cryptographic Module Specification

This section defines those requirements for identifying and establishing the cryptographic boundary of the module. This includes the specification of the hardware, software, and/or firmware; the module interfaces; manual or logical controls; identification of the implemented algorithms and modes of operation; and the module's security policy.

The primary modification to this section is the inclusion of the approved cryptographic algorithms and security functions. FIPS 140-1 separated the algorithm identification into a short standalone section. However, given that the cryptographic algorithm is the basis of the module, inclusion of the algorithm specification in the first section of FIPS 140-2 was a logical restructuring.

2.1.2. Cryptographic Module Ports and Interfaces

This section defines the requirements used to restrict information flow and physical access to the logical interfaces for all entry and exit points both internal and external to the module. The standard defines four specific logical interfaces including data input, data output, control input, and status output, and the associated requirements by security level.

The major change in this section involves the underlying requirement for plaintext input/output (I/O) to be separated from other types of I/O. FIPS 140-1 met this requirement by specifying the use of physically separate ports beginning at security level 3 for plaintext I/O. Due to changes in technology (e.g., timing separation, dedicated threads, multiplexing, etc.), the standard now allows both physically separate ports and logical separation within existing physical ports via trusted path.

2.1.3. Roles, Services, and Authentication

This section is divided into three subsections covering the requirements for the authorized operator roles; services, functions and operations provided by the module; and the authentication needed to obtain these services.

The major modification to this section is the addition of strength of mechanism requirements for authentication. This represents a strengthening of the standard and the first time the concept of strength of mechanism has been specified. These new requirements address minimum probabilities for guessing authentication data (e.g., pins, passwords, etc.), false acceptance error rates and restrictions placed on the feedback of authentication data to the user.

2.1.4. Finite State Model

This section specifies the underlying design requirements for the identification and specification of the module's operational and error states and associated transitions between states. The name of this section was changed from Finite State Machine (FSM) to Finite State Model to more accurately reflect the requirements. FIPS 140-1 mandated the use of an FSM Model in the module's design. The FSM is often associated with hardware design and development. To better represent both hardware and software modules, this section now includes the concept of utilizing a Finite State Model or an equivalent design methodology.

2.1.5. Physical Security

This section details all of the requirements surrounding the physical security of the cryptographic module. Cryptographic modules are separated into three different embodiment categories: single chip, multi-chip embedded, and multi-chip standalone.

The majority of changes to this section involve a re-organization of the sub-sections that define the requirements for the three different module embodiments. FIPS 140-1 was structured with a separate section of requirements for each of three module embodiments, plus a subsection detailing the Environmental Failure Protection (EFP)/Environmental Failure Testing (EFT) requirements for security level 4. For consistency and clarity, FIPS 140-2 moves all of the redundant requirements from the three embodiments into a general section defining requirements applicable to all. The requirements that are unique to each of the embodiments follow the general section concluding with EFP/EFT. In addition to the restructuring, new requirements were added for single chip and multi-chip embedded modules to allow the use of physical enclosures for the protection of the module.

2.1.6. Operational Environment

This section details the requirement specific to modules where an operator can load and execute software or firmware that was not included as part of the module validation. An example of a cryptographic module for which the operational environment requirements apply is a general-purpose computer running cryptographic software as well as untrusted user-supplied software (e.g., a spreadsheet or word processing program). In this case, the hardware, operating system, and cryptographic software are considered part of the module. FIPS 140-2 relies on an evaluated operating system to mitigate part of the security concerns over “Trojan Horse” attacks, where the user-supplied software or firmware can access, obtain, or corrupt the module’s critical security parameters (e.g., cryptographic keys, passwords, etc.).

The major modification to this section was the replacement of criteria for evaluating operating systems. FIPS 140-1 required evaluated operating systems that referenced the Trusted Computer System Evaluation Criteria (TCSEC) classes C2, B1 and B2. The TCSEC is no longer in use and has been replaced by the Common Criteria. Consequently, FIPS 140-2 now references the *Common Criteria for Information Technology Security Evaluation* (CC), ISO/IEC 15408:1999.

2.1.7. Cryptographic Key Management

This section contains the security requirements for cryptographic key management that encompasses the entire lifecycle of the cryptographic keys used by a cryptographic module. This includes random number generation, key generation, establishment, entry/output, storage, and zeroization. The requirements are applicable to modules that implement secret key and/or public key algorithms.

The major modification to this section was the addition of requirements for Over-The-Air-Rekeying (OTAR) for radio communication modules. Other modifications included: clarification of the deterministic and nondeterministic random number generators (RNGs) sub-section to allow RNGs approved for classified processing for use in key generation; addition of strength of mechanism requirements in the Key Establishment subsection; and the deletion of the Key Archive sub-section.

2.1.8. Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC)

This section specifies the Federal Communications Commission (FCC) requirements applicable to cryptographic modules. These requirements are specific to the module’s ability to operate in a

manner that does not interfere electromagnetically with other devices. Requirements necessary to mitigate cryptographic attacks based on electromagnetic emanations (TEMPEST) are not included in this section. The Mitigation of Other Attacks section of the standard contains the requirements related to TEMPEST attacks.

During the update process, the EMI/EMC section was modified to reflect minor changes in FCC requirements and references.

2.1.9. Self-Tests

This section provides the requirements necessary to ensure that the module is functioning properly. Self-testing is required at both module power-up and when specific conditions are met. These tests include public/private key generation, software/firmware loading, manual key entry, random number generation, and cryptographic bypass (plaintext in, plaintext out).

The update to the standard resulted in no dramatic change in scope or format for self-test requirements; however, previously issued guidance was included. The major changes in the Self-Test section were strengthening the required tests and better addressing the bypass mode of operation. To strengthen the requirements, the new standard now mandates all four statistical random number generator tests. FIPS 140-1 only required one of the four. Further, the statistical limits for passing these tests were tightened to provided additional assurance for random number generation. Public comments recommended that the Self-Test section better address modules (i.e., routers) that are designed to automatically switch between bypass and secure mode (plaintext in, ciphertext out). This was accomplished by including requirements specific to the secure operation of the module during the switch between modes. These new requirements facilitate the underlying requirement of fail-secure, where plaintext information is not released inadvertently. In addition, FIPS 140-1 tested bypass capabilities only at module power-up. The new standard moves bypass to the conditional testing area.

2.1.10. Design Assurance

The Design Assurance section, which was formerly Software Security in FIPS 140-1, defines the requirements for configuration management, delivery and operation, development and guidance documents. The intent of this section is to provide security assurance from design and development of the module through delivery and initial start-up.

Originally this section only specified requirements for software, but to provide greater security assurance the section has now been expanded to address software, hardware, and firmware. Though the entire section was re-written, the consolidated design assurance requirements found in FIPS 140-1 forms the base. These requirements included reviews of source code, functional specifications, and formal modeling. Requirements new to the standard include configuration management, correct delivery and start-up, and mandatory guidance documents for users and cryptographic officers.

2.1.11. Mitigation of Other Attacks

This section is the first new section of the standard and provides information, recommendations, and requirements for several new types of cryptographic attacks. Susceptibility to these attacks depends on module type, implementation, and implementation environment. These attacks are of particular concern for cryptographic modules implemented in hostile environments or where the attackers may be the users of the module. Generally, these types of attacks rely on the analysis of information obtained from sources physically external to the module. In all cases, the attacks attempt to determine some knowledge about the cryptographic keys and critical security parameters (CSPs) contained in the module. This section was developed as a direct result of numerous public comments recommending that power analysis, timing analysis, fault induction,

and TEMPEST attacks be addressed by FIPS 140-2. Certain types of cryptographic modules may be susceptible to these attacks (e.g., tests for power analysis, timing analysis, and fault induction), but testable security requirements were not available at the time this standard was issued or the attacks were outside of the scope of the standard (e.g., TEMPEST attacks). The new standard specifies that if a cryptographic module is designed to mitigate one or more specific attacks, then the module's security policy shall specify the security mechanisms employed by the cryptographic module to mitigate the attack(s). The existence of these mechanisms and their proper functioning will be validated when requirements and associated tests are developed. Brief summaries of currently known attacks are provided in the standard.

2.1.12. Appendixes

FIPS 140-1 contains three appendixes, A, B, and D below. Appendix C has been added to FIPS 140-2.

A. *Summary of Documentation Requirements*

This section was updated to reflect modifications in the standard.

B. *Recommended Software Development Practices*

This section was updated to reflect current practices.

C. *Security Policy*

Appendix C specifies the information and structure of the required cryptographic module security policy. This document is available by request and often provides the only information users have access to prior to purchasing the module. FIPS 140-1 required a security policy, which contained the security rules of the module. However, no format or specific content requirements were mandated. Therefore cryptographic module security policies submitted by vendors often varied greatly in detail and quality. FIPS 140-2 mandates more stringent requirements for both the contents of a security policy and the structure. The vendors now must provide information concerning the identification and authentication, access control, and physical security mechanisms, and any mechanisms implemented for mitigation of other attacks. Two types of security policies may exist. A proprietary security policy used by the testing laboratory to perform necessary tests and a required non-proprietary version, which is available to public release.

D. *Selected Bibliography*

This section was updated to reflect current standards and documents.

3. DETAILED DIFFERENCES BETWEEN FIPS 140-1 AND FIPS 140-2

This section summarizes the documentation and terminology changes and lists the specific requirements changes by section of FIPS 140-2.

3.1. Documentation Requirements

In all security requirement areas, FIPS 140-2 explicitly specifies requirements for documentation by the vendor of a cryptographic module. Some of these documentation requirements are implicit in FIPS 140-1 (being made explicit by requirements for conformance testing). In this comparison, differences are noted only for those cases where FIPS 140-2 requires documentation that is new or is a notable extension of the requirements in FIPS 140-1.

3.2. Noteworthy Differences in Terminology

Changes have been made to the terminology so that the Standard may be easily adapted by other standards bodies. In particular, in FIPS 140-2, the terms “Approved” (used only in capitalized form) and “Approved security functions” are adopted in place of the corresponding FIPS 140-1 terms “FIPS-Approved” and “FIPS approved security method.”

The supporting FIPS 140-2 definitions are:

> *Approved*: FIPS-Approved and/or NIST-recommended.
>
> *Approved security function:* for this standard, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either
> (a) specified in an Approved standard,
> (b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or
> (c) specified in the list of Approved security functions.

Other standards bodies need only to re-define “Approved”, without having to make significant changes to the body of the standard.

> FIPS 140-2 is explicit in stating that for purpose of validation a cryptographic module is required to implement at least one Approved security function used in an *Approved mode of operation*: a mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., DES CBC mode).

(Other algorithms or security functions may also be included for use in non-Approved modes of operation in a cryptographic module but will not be tested in the validation process.)

3.3. Differences in Specific Security Requirement Areas

This section lists the specific requirements included in FIPS 140-1 and the associated revised (or new) requirements included in FIPS 140-2. (Note: the format of the FIPS 140-2 requirements included in this document may vary from the standard for ease of reviewing.)

3.3.1. Cryptographic Module Specification

The area has been renamed (from *Cryptographic Modules* in FIPS 140-1 to *Cryptographic Module Specification* in FIPS 140-2) to more accurately reflect the content of the material.

The FIPS 140-1 definition of cryptographic module:

> (Levels 1, 2, 3, and 4) “A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof, that implements cryptographic logic or processes.”

has been clarified in FIPS 140-2:

> (Levels 1, 2, 3, and 4) “ A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.”

The FIPS 140-1 definition of a cryptographic boundary:

> (Levels 1, 2, 3, and 4) “If a cryptographic module contains software or firmware, the cryptographic boundary shall be defined such that it contains the processor which executes the code.”

has been clarified in FIPS 140-2:

> (Levels 1, 2, 3, and 4) “If A cryptographic boundary shall consist of an explicitly defined perimeter that establishes the physical bounds of a cryptographic module.”

The contents of the FIPS 140-1 Section entitled “Cryptographic Algorithms,” consisting of the single statement:

> (Levels 1, 2, 3, and 4) “Cryptographic modules shall employ FIPS-approved cryptographic algorithms.”

has been subsumed by this section of FIPS 140-2 in the following requirements:

> (Levels 1, 2, 3, and 4) “A cryptographic module shall implement at least one Approved security function used in an Approved mode of operation.”
>
> (Levels 1, 2, 3, and 4) “The operator shall be able to determine when an Approved mode of operation is selected.”
>
> (Levels 1 and 2) “The cryptographic module security policy may specify when a cryptographic module is performing in an Approved mode of operation.”
>
> (Levels 3 and 4) “A cryptographic module shall indicate when an Approved mode of operation is selected. (Approved security functions are listed in Annex A to this standard.)”
>
> (Levels 1, 2, 3, and 4) “Documentation shall list all security functions, both Approved and non-Approved, that are employed by a cryptographic module and shall specify all modes of operation, both Approved and non-Approved.”

FIPS 140-2 is more explicit in its requirements for general documentation of hardware, software and and firmware components. The FIPS 140-1 requirement (moved from the section entitled “Software Security”):

> (Levels 1, 2, 3, and 4) “Documentation shall include a detailed description of the design of software within the module”

has been extended in FIPS 140-2:

> (Levels 1, 2, 3, and 4) "Documentation shall specify the design of the hardware, software, and firmware components of a cryptographic module. High-level specification languages for software/firmware or schematics for hardware should be used to document the design."

FIPS 140-2 explicitly requires documentation of information contained in cryptographic modules that must be protected:

> (Levels 1, 2, 3 and 4) "Documentation shall specify all security-related information, including secret and private cryptographic keys (both plaintext and encrypted), authentication data (e.g., passwords, PINs), other CSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module."

Documentation requirements involving interfaces to the cryptographic module, manual and logical controls, and physical or logical status indicators, that appear in "Module Interfaces" area of FIPS 140-1, have been moved without substantive modification to this area of FIPS 140-2.

3.3.2. Cryptographic Module Ports and Interfaces

This area has been renamed (from *Module Interfaces* in FIPS 140-1 to *Cryptographic Module Ports and Interfaces* in FIPS 140-2) to more accurately reflect the content of the material.

The security requirements involving a "maintenance access interface" and a "maintenance access role", specified in Section 2 (*Module Interfaces*) of FIPS 140-1, have been moved to the *Physical Security* and *Roles, Services, and Authentication*, areas of FIPS 140-2.

The higher security level requirements involving the ports used for the input and output of plaintext security-relevant data have been revised. Specifically, the FIPS 140-1 requirements:

> (Levels 3 and 4) "The data input and output port or ports used for plaintext cryptographic key components, plaintext authentication data, and other unprotected critical security parameters shall be physically separated from all other ports of the module. Furthermore, these ports shall allow for direct entry of plaintext cryptographic key components, plaintext authentication data, and other unprotected critical security parameters, as required in Section 4.8.3."

have been replaced in FIPS 140-2 by:

> (Levels 3 and 4)
> - "The physical port(s) used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be physically separated from all other ports of the cryptographic module
>
> or
>
> - the logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path,
>
> and
>
> - plaintext cryptographic key components, authentication data, and other CSPs shall be directly entered into the cryptographic module (e.g., via a trusted path or directly attached cable). (See Section 4.7.4.)"

3.3.3. Roles, Services, and Authentication

The area has been renamed (from *Roles and Services* in FIPS 140-1 to *Roles, Services, and Authentication* in FIPS 140-2) to more accurately reflect the content of the material.

3.3.3.1. Roles

There are no major changes to the requirements in this subsection.

3.3.3.2. Services

In addition to the "Show Status" and "Perform Self-Tests" services, FIPS 140-2 explicitly requires the following service of a cryptographic module:

> *Perform Approved Security Function*: Perform at least one Approved security function used in an Approved mode of operation.

In FIPS 140-2, for cryptographic modules that implement a bypass capability, the "Show Status" indicator must also indicate an alternating state. Specifically, the requirement in FIPS 140-1:

> (Levels 1, 2, 3, and 4) "If a cryptographic module implements a bypass capability, then the current status of the module (e.g., the response to a 'Show Status' service request) shall indicate whether or not the bypass capability is activated."

has been replaced by the following requirement in FIPS 140-2:

> (Levels 1, 2, 3, and 4) "If a cryptographic module implements a *bypass* capability, where services are provided without cryptographic processing (e.g., transferring plaintext through the module without encryption), then
>
> - the module shall show status to indicate whether
>
> 1) the bypass capability *is not* activated, and the module is exclusively providing services *with* cryptographic processing (e.g., plaintext data *is* encrypted),
>
> 2) the bypass capability *is* activated and the module is exclusively providing services *without* cryptographic processing (e.g., plaintext data *is not* encrypted), or
>
> 3) the bypass capability *is alternately* activated and deactivated and the module is providing some services *with* cryptographic processing and some services *without* cryptographic processing (e.g., for modules with multiple communication channels, plaintext data *is* or *is not* encrypted depending on each channel configuration)."

FIPS 140-2 also requires the vendor to specifically cite the services that can be performed by a module for an operator who does not assume a role supported by the module:

> (Levels 1, 2, 3, and 4) "Documentation shall specify any services provided by the cryptographic module for which the operator is not required to assume an authorized role, and how these services do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the module."

3.3.3.3. Operator Authentication

Implicit in FIPS 140-1, FIPS 140-2 explicitly requires the identification of "other means" to control

"initial" crypto-officer access to the cryptographic module:

> (Levels 1,2, 3, and 4) "If a cryptographic module does not contain the authentication data required to authenticate the operator for the first time the module is accessed, then other authorized methods (e.g., procedural controls or use of factory-set or default authentication data) shall be used to control access to the module and initialize the authentication mechanisms."

FIPS 140-2 specifies requirements for the strength of authentication mechanisms for a cryptographic module:

> - (Levels 2, 3, and 4) "For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods)."
> - (Levels 2, 3, and 4) "For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur."
> - (Levels 2, 3, and 4) "Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password)."
> - (Levels 2, 3, and 4) "Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism."

> (Levels 1, 2, 3, and 4) "Documentation shall specify:
>
> - the authentication mechanisms supported by a cryptographic module,
> - the types of authentication data required by the module to implement the supported authentication mechanisms,
> - the authorized methods used to control access to the module for the first time and initialize the authentication mechanisms, and
> - the strength of the authentication mechanisms supported by the module."

For Security Level 1, a cryptographic module is not required to employ authentication mechanisms to control access to the module. In this case, FIPS 140-2 requires the following:

> (Security Level 1) "If authentication mechanisms are not supported by a cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator."

3.3.4. Finite State Model

The area has been renamed (from *Finite State Machine Model* in FIPS 140-1 to *Finite State Model* in FIPS 140-2).

The FIPS 140-1 requires a correspondence between a "maintenance access interface" and corresponding finite state machine "maintenance states." This is modified in FIPS 140-2 by a requirement of a correspondence between a "maintenance role" and "maintenance states." More precisely, the FIPS 140-1 requirement:

(Levels 1, 2, 3, and 4) “If a cryptographic module contains a maintenance access interface, then it shall include maintenance states.”

has been replaced by the FIPS 140-2 requirement:

(Levels 1, 2, 3, and 4) “If a cryptographic module contains a maintenance role, then a maintenance state shall be included.”

3.3.5. Physical Security

The security requirements in this area have been reorganized to eliminate the redundancies found in FIPS 140-1. A new subsection entitled *General Security Requirements* captures for each security level those requirements that are applicable to all three physical embodiments: single-chip, multiple-chip embedded, and multiple-chip standalone cryptographic modules.

Most of the discussion on the maintenance access interface, found in the area entitled *Module Interfaces* of FIPS 140-1, has been moved to this area of FIPS 140-2.

FIPS 140-2 clarifies the lower security level requirements for (procedural and automatic) zeroization of plaintext secret and private keys and other CSPs when performing physical maintenance:

(Levels 1 and 2) “When performing physical maintenance, all plaintext secret and private keys and other unprotected CSPs contained in the cryptographic module shall be zeroized. Zeroization shall either be performed procedurally by the operator or automatically by the cryptographic module.”

The documentation requirements have been extended to include how the zeroization takes place when accessing the maintenance access interface.

(Level 1, 2, 3, and 4) “Documentation shall specify the maintenance access interface and how plaintext secret and private keys and CSPs are zeroized when the maintenance access interface is accessed.”

At Security Level 2 in FIPS 140-2, the physical embodiments for multiple-chip embedded cryptographic modules have been extended to include the use of a tamper-evident *enclosure* as an alternative to the use of a tamper-evident *coating*.

3.3.6. Operational Environment

This area has been renamed (from *Operating System Security* in FIPS 140-1 to *Operational Environment* in FIPS 140-2) to more accurately reflect the content of the material.

The substantive changes made to the operating system requirements involve:

- Adoption of Recommended CC Protection Profiles functional requirements evaluated at Evaluation Assurance Level (EAL) 2 with additional functional and assurance requirements (in place of the TCSEC C2, B1, and B2 functional and assurance requirements). (Note that TCSEC labeling requirements are no longer required for Security Levels 3-4.)

- Discretionary access control mechanisms that are explicitly role-based as opposed to

operator and/or process-based, and

- Requirements for audit capabilities and run-time auditing.

General

The criteria for applicability of the operating system requirements has been expanded in FIPS 140-2. In particular, the FIPS 140-1 requirement:

> (Levels 1, 2, 3, and 4) "The operating systems requirements in this section apply to a cryptographic module only if the module provides a means whereby and operator can load and execute software or firmware that was not included as part of the validation of the module."

has been replaced by the FIPS 140-2 requirements:

> (Levels 1, 2, 3, and 4) "If the operational environment is a modifiable operational environment, the operating system requirements in Section 4.6.1 shall apply. If the operational environment is a limited operational environment, the operating system requirements in Section 4.6.1 do not apply. A *limited operational environment* refers to a static non-modifiable virtual operational environment (e.g., JAVA virtual machine or a non-programmable PC card) with no underlying general purpose operating system upon which the operational environment uniquely resides."

FIPS 140-2 is explicit in documentation requirements regarding the strength of the operating system:

> (Levels 1, 2, 3, and 4) "Documentation shall specify the operational environment for a cryptographic module, including, if applicable, the operating system employed by the module, and for Security Levels 2, 3, and 4, the Protection Profile and the CC assurance level."

Security Level 1

The FIPS 140-1 requirements that exclude the use of multiuser, multiprocess systems:

> (Level 1 only) "Use of the cryptographic module shall be limited to a single user at a time."
>
> (Level 1 only) "Use of the cryptographic module shall be dedicated to the cryptographic process during the time the cryptographic process is in use."

have been replaced by a set of requirements that achieve the same security within the context of current multiprocess operating systems:

> (Level 1 only) "The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded)."
>
> (Level 1 only) "The cryptographic module shall prevent access by other processes to plaintext private and secret keys, CSPs, and intermediate key generation values during the time the cryptographic module is executing/operational. Processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators. Non-cryptographic processes shall not interrupt a cryptographic module during execution."

The FIPS 140-1 requirements on the internal storage of cryptographic software have been generalized in FIPS 140-2 and extended to include firmware. Specifically, the FIPS 140-1

requirement:

> (Levels 1, 2, 3, and 4) "All cryptographic software shall be installed only as executable code in order to discourage scrutiny and modification by users."

has been replaced in FIPS 140-2 by:

> (Levels 1, 2, 3, and 4) "All cryptographic software and firmware shall be installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification."

The application of an Approved integrity technique for software has been extended in FIPS 140-2 to also include firmware. Specifically, the FIPS 140-1 requirement:

> (Levels 1, 2, 3, and 4) "A cryptographic mechanism using a FIPS approved authentication technique (e.g., the computation and verification of a data authentication code or NIST digital signature algorithm) shall be applied to the cryptographic software within the cryptographic module."

has been replaced in FIPS 140-2 by:

> (Levels 1, 2, 3, and 4) "A cryptographic mechanism using an Approved integrity technique (e.g., an Approved message authentication code or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the cryptographic module."

Security Level 2

In FIPS 140-2, the functional security requirements of the OS are those specified by the Recommended Protection Profiles evaluated at the CC EAL2. More precisely, the FIPS 140-1 requirements:

> (Level 2 Only) "All cryptographic software, cryptographic keys and other critical security parameters, and control and status information shall be under the control of an operating system that provides controlled access protection (i.e., C2 protection in accordance with the Trusted Computer System Evaluation Criteria (TCSEC), or FIPS approved equivalent). Only operating systems that have been evaluated by a NIST accredited evaluation authority and against a FIPS approved criteria shall be used."

have been replaced by the FIPS 140-2 requirements:

> (Level 2 Only) "All cryptographic software and firmware, cryptographic keys and CSPs, and control and status information shall be under the control of
>
> - an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B and is evaluated at the CC evaluation assurance level EAL2, or
> - an equivalent evaluated trusted operating system."

The discretionary access control mechanisms of an OS have been clarified in FIPS 140-2 as being "role based" rather than "operator and/or process based" in FIPS 140-1. The applicable FIPS 140-2 requirements are as follows:

(Levels 2, 3, and 4) “To protect plaintext data, cryptographic software and firmware, cryptographic keys and CSPs, and authentication data, the discretionary access control mechanisms of the operating system shall be configured to specify the set of roles that can

- *execute* stored cryptographic software and firmware,
- *modify* (i.e., write, replace, and delete) the following cryptographic module software or firmware components stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., cryptographic keys and audit data), CSPs, and plaintext data,
- *read* the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., cryptographic keys and audit data), CSPs and plaintext data and
- *enter* cryptographic keys and CSPs.”

The FIPS 140-1 requirements for OS audit capabilities at Security Levels 3 and 4 have been extended to Security Level 2 in FIPS 140-2:

(Levels 2, 3, and 4) “The operating system shall provide an audit mechanism to record modifications, accesses, deletions, and additions of cryptographic data and CSPs.”

FIPS 140-2 specifies the set of events that must be must be audited by the OS:

(Levels 2, 3, and 4) “The following events shall be recorded by the audit mechanism:

- attempts to provide invalid input for crypto officer functions, and
- the addition or deletion of an operator to/from a crypto officer role.”

FIPS 140-2 specifies the set of events that must be auditable by the OS:

(Levels 2, 3, and 4) “The audit mechanism shall be capable of auditing the following events:

- operations to process audit data stored in the audit trail,
- requests to use authentication data management mechanisms,
- use of a security-relevant crypto officer function,
- requests to access user authentication data associated with the cryptographic module,
- use of an authentication mechanism (e.g., login) associated with the cryptographic module,
- explicit requests to assume a crypto officer role, and
- the allocation of a function to a crypto officer role.”

Security Level 3

In FIPS 140-2, the functional security requirements of the OS are those specified by the Recommended Protection Profiles evaluated at the CC EAL3. More precisely, the FIPS 140-1 requirements:

(Level 3) “All cryptographic software, cryptographic keys and other critical security parameters, control and status information shall be labeled and under the control of an operating system that provides labeled protection (i.e., B1 protection in accordance with the Trusted Computer System Evaluation Criteria (TCSEC), or FIPS approved equivalent). Only operating systems that have been evaluated by a NIST accredited evaluation authority and against a FIPS approved criteria shall be used.”

have been replaced by the FIPS 140-2 requirements:

> (Level 3) "All cryptographic software and firmware, cryptographic keys and CSPs, and control and status information shall be under the control of
>
> - an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B. The operating system shall be evaluated at the CC evaluation assurance level EAL3 and include the following additional requirements: Trusted_Path (FTP_TRP.1) and Informal TOE Security Policy Model (ADV_SPM.1), or
>
> - an equivalent evaluated trusted operating system."

The TCSEC terminology of a Trusted Computing Base (TCB) in FIPS 140-1 has been changed to the CC terminology of a Target of Evaluation Security Functions (TSF):

> (Levels 3 and 4) "All cryptographic keys and CSPs, authentication data, control inputs, and status outputs shall be communicated via a trusted mechanism (e.g., a dedicated I/O physical port or a trusted path). If a trusted path is used, the Target of Evaluation Security Functions (TSF) shall support the trusted path between the TSF and the operator when a positive TSF-to-operator connection is required. Communications via this trusted path shall be activated exclusively by an operator or the TSF and shall be logically isolated from other paths."

FIPS 140-2 specifies events that must be audited by the OS:

> (Levels 3 and 4) "In addition to the audit requirements of Security Level 2, the following events shall be recorded by the audit mechanism:
>
> - attempt to use the trusted path function, and
> - Identification of the initiator and target of a trusted path."

Security Level 4

In FIPS 140-2, the functional security requirements of the OS are those specified by the Recommended Protection Profiles evaluated at the CC EAL4. More precisely, the FIPS 140-1 requirements:

> (Level 4) "All cryptographic software, cryptographic keys and other critical security parameters, control and status information shall be labeled and under the control of an operating system that provides structured protection (i.e., B2 protection in accordance with the Trusted Computer System Evaluation Criteria (TCSEC), or FIPS approved equivalent). Only operating systems that have been evaluated by a NIST accredited evaluation authority and against a FIPS approved criteria SHALL be used."

have been replaced by the FIPS 140-2 requirements:

> (Level 4) "All cryptographic software, cryptographic keys and CSPs, and control and status information shall be under the control of
>
> - an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B. The operating system shall be evaluated at the CC evaluation assurance level EAL4, or
>
> - an equivalent evaluated trusted operating system."

3.3.7. Cryptographic Key Management

The requirements for *Key Archiving* (Section 4.8.6 in FIPS 140-1) have been eliminated in FIPS 140-2.

The documentation requirements have been explicitly specified in FIPS 140-2:

> (Levels 1, 2, 3, and 4) "Documentation shall specify all cryptographic keys, cryptographic key components, and CSPs employed by a cryptographic module."

3.3.7.1. Random Number Generators (RNGs)

FIPS 140-2 specifies security requirements for cryptographic modules that implement deterministic and/or nondeterministic random number generators (RNGs).

> (Levels 1, 2, 3, and 4) "If a cryptographic module employs Approved or non-Approved RNGs in an Approved mode of operation, the data output from the RNG shall pass the continuous random number generator test as specified in Section 4.9.2. Depending on the security level, the data output from an Approved RNG shall pass all statistical tests for randomness as specified in Section 4.9.1. Approved deterministic RNGs shall be subject to the cryptographic algorithm test in Section 4.9.1. Approved RNGs are listed in Annex C to this standard."
>
> (Levels 1, 2, 3, and 4) "Until such time as an Approved nondeterministic RNG standard exists, nondeterministic RNGs approved for use in classified applications may be used for key generation or to seed Approved deterministic RNGs used in key generation. Commercially available nondeterministic RNGs may be used for the purpose of generating seeds for Approved deterministic RNGs. Nondeterministic RNGs shall comply with all applicable RNG requirements of this standard."
>
> (Levels 1, 2, 3, and 4) "An Approved RNG shall be used for the generation of cryptographic keys used by an Approved security function. The output from a non-Approved RNG may be used 1) as input (e.g., seed, and seed key) to an Approved deterministic RNG or 2) to generate initialization vectors (IVs) for Approved security function(s). The seed and seed key shall not have the same value."
>
> (Levels 1, 2, 3, and 4) "Documentation shall specify each RNG (Approved and non-Approved) employed by a cryptographic module."

3.3.7.2. Key Generation

FIPS 140-2 allows only Approved RNGs to be used in the key generation process. Specifically, the FIPS 140-1 requirement:

> (Levels 1, 2, 3, and 4) "When a random number is used in the key generation process, all values shall be generated randomly or pseudorandomly such that all combinations of bits and all possible values are equally likely to be generated."

has been replaced in FIPS 140-2 by:

> (Levels 1, 2, 3, and 4) "If an Approved key generation method requires input from a RNG, then an Approved RNG that meets the requirements specified in Section 4.7.1 shall be used."

FIPS 140-2 specifies security requirements regarding the general compromise of the key generation algorithm:

(Levels 1, 2, 3, and 4) “Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic RNG) shall require at least as many operations as determining the value of the generated key.”

FIPS 140-2 is explicit in the manner in which intermediate key generation values can be output by a cryptographic module. Specifically, the FIPS 140-1 requirement:

(Levels 1, 2, 3, and 4) “If intermediate key generation states and values shall not be accessible outside of the module in plaintext or otherwise unprotected form.”

has been replaced by the FIPS 140-2 requirement:

(Levels 1, 2, 3, and 4) “If intermediate key generation values are output from the cryptographic module, the values shall be output either 1) in encrypted form or 2) under split knowledge procedures.”

3.3.7.3. Key Establishment

In FIPS 140-1, this subsection is entitled *Key Distribution*.

FIPS 140-2 specifies security requirements for establishing cryptographic keys using radio communications:

(Levels 1, 2, 3, and 4) “If, in lieu of an Approved key establishment method, a radio communications cryptographic module implements Over-The-Air-Rekeying (OTAR), it shall be implemented as specified in the TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, Over-The-Air-Rekeying (OTAR) Protocol, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA, January, 1996, Telecommunications Industry Association.”

FIPS 140-2 specifies security requirements regarding the general compromise of the key establishment method:

(Levels 1, 2, 3, and 4) “Compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require at least as many operations as determining the value of the cryptographic key being transported or agreed upon.”

3.3.7.4. Key Entry and Output

FIPS 140-2 specifies the manner for entering and outputting cryptographic keys:

(Levels 1, 2, 3, and 4) “If cryptographic keys are entered into or output from a cryptographic module, the entry or output of keys shall be performed using either manual (e.g., via a keyboard) or electronic methods (e.g., smart cards/tokens, PC cards, or other electronic key loading devices).”

(Levels 1, 2, 3, and 4) “A seed key, if entered during key generation, shall be entered in the same manner as cryptographic keys.”

If secret and private keys are themselves encrypted, FIPS 140-2 requires that an Approved algorithm be used:

(Levels 1, 2, 3, and 4) “All encrypted secret and private keys, entered into or output from a cryptographic module and used in an Approved mode of operation, shall be encrypted using an Approved algorithm.”

When split knowledge procedures are used to enter or output secret and private keys, FIPS 140-2 specifies requirements for the key components:

(Levels 3 and 4) “If split knowledge procedures are used:

- the cryptographic module shall separately authenticate the operator entering or outputting each key component,
- plaintext cryptographic key components shall be directly entered into or output from the cryptographic module (e.g., via a trusted path or directly attached cable) without traveling through any enclosing or intervening systems where the key components may inadvertently be stored, combined, or otherwise processed (see Section 4.2),
- at least two key components shall be required to reconstruct the original cryptographic key,
- documentation shall prove that if knowledge of *n* key components is required to reconstruct the original key, then knowledge of any *n*-1 key components provides no information about the original key other than the length, and
- documentation shall specify the procedures employed by a cryptographic module.”

3.3.7.5. Key Storage

FIPS 140-2 clarifies the storing of secret and private keys in a cryptographic module. In particular, the FIPS 140-1 requirement:

> (Levels 1, 2, 3, and 4) “When contained within a cryptographic module, secret and private keys may be stored in plaintext form.”

has been replaced in FIPS 140-2 by the requirement:

(Levels 1, 2, 3, and 4) “Cryptographic keys stored within a cryptographic module shall be stored either in plaintext form or encrypted form.”

3.3.7.6. Key Zeroization

This subsection was entitled *Key Destruction* in FIPS 140-1.

3.3.8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Reference to the specific subparts of the *47 Code of Federal Regulations* for EMI/EMC requirements have been updated in FIPS 140-2:

(Levels 1 and 2) “A cryptographic module shall (at a minimum) conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).”

(Levels 3 and 4) “A cryptographic module shall (at a minimum) conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).”

3.3.9. Self-Tests

FIPS 140-2 is explicit in the documentation requirements:

(Levels 1, 2, 3, and 4) “Documentation shall specify:

- the self-tests performed by a cryptographic module, including power-up and conditional tests,
- the error states that a cryptographic module can enter when a self-test fails, and
- the conditions and actions necessary to exit the error states and resume normal operation of a cryptographic module (i.e., this may include maintenance of the module, or returning the module to the vendor for servicing.”

3.3.9.1. Power-up Tests

Cryptographic algorithm test

The application of the cryptographic algorithms test has been clarified. More precisely, the FIPS 140-1 requirement:

> (Levels 1, 2, 3, and 4) “A known answer test shall be run for each cryptographic function (e.g., encryption, decryption, authentication) that is implemented.”

has been replaced in FIPS 140-2 by:

(Levels 1, 2, 3, and 4) “A cryptographic algorithm test using a known answer shall be conducted for all modes (e.g., encryption, decryption, authentication, and deterministic random number generation) of each Approved cryptographic algorithm implemented by a cryptographic module.”

(Levels 1, 2, 3, and 4) “Cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the Digital Signature Algorithm) shall be tested using a known-answer test or shall be tested using a pair-wise consistency test.”

Software/firmware integrity test

In applying the software/firmware integrity test, a lower bound has been placed on the size of the error detection code:

(Levels 1, 2, 3, and 4) “If an EDC is used, the EDC shall be at least 16 bits in length.”

Statistical random number generator tests

The four statistical random number tests, recommended in FIPS 140-1 with the possibility of substituting alternative equivalent or superior tests, are required without exception in FIPS 140-2. Specifically, the FIPS 140-2 requirement is:

(Levels 3 and 4) “A single bit stream of 20,000 consecutive bits of output from each RNG shall be subjected to the following four tests: monobit test, poker test, runs test, and long runs test.”

The acceptance intervals for each of the statistical random number tests have been revised to decrease the probability of a false acceptance for a single bit stream of 20,000 consecutive bits of output:

- Monobit Test: (9,725 < X < 10,275) for the number of 1’s.
- Poker Test: (2.16 < X < 46.17) for the stated measure.
- Runs Test:

Length of Run	Required Interval
1	2,343 – 2,657
2	1,135 – 1,365
3	542 - 708
4	251 - 373
5	111 - 201
6+	111 - 201

- Long Runs Test: a long run is defined to be of length 26 or more (of either zeros or ones).

3.3.9.2. Conditional Tests

Pairwise consistency test

The following requirement involving key agreement is new in FIPS 140-2:

(Levels 1, 2, 3, and 4) “If the keys are to be used to perform key agreement, then the cryptographic module shall create a second, compatible key pair. The cryptographic module shall then perform both sides of the key agreement algorithm and shall compare the resulting shared values. If the shared values are not equal the test shall fail.”

Manual key entry test

The following new requirement in FIPS 140-2 applies to keys or key components that are manually entered into a cryptographic module:

(Levels 1, 2, 3, and 4) “If an EDC is used, the EDC shall be at least 16 bits in length.”

Bypass test

The following requirements have been in added in FIPS 140-2 for cryptographic modules that implement a bypass test:

(Levels 1, 2, 3, and 4) “If a cryptographic module implements a *bypass* capability where the services may be provided without cryptographic processing (e.g., transferring plaintext through the module), then the following bypass tests shall be performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext:

1. A cryptographic module shall test for the correct operation of the services providing

cryptographic processing when a switch takes place between an exclusive bypass service and an exclusive cryptographic service.

2. If a cryptographic module can automatically alternate between a bypass service and a cryptographic service, providing some services *with* cryptographic processing and some services *without* cryptographic processing, then the module shall test for the correct operation of the services providing cryptographic processing when the mechanism governing the switching procedure is modified (e.g., an IP address source/destination table). "

(Levels 1, 2, 3, and 4) "Documentation shall specify the mechanism or logic governing the switching procedure."

3.3.10. Design Assurance

This area has been renamed (from *Software Security* in FIPS 140-1 to *Design Assurance* in FIPS 140-2) to more accurately reflect the content of the material. New security requirements are specified for the following subsections:

- Configuration Management – provides assurance that the functional requirements and specifications are realized in the implementation of a cryptographic module.
- Delivery and Operation – provides assurance that a cryptographic module is securely delivered to authorized operators, and is installed and initialized in a correct and secure manner.
- Development – provides assurance that the implementation of a cryptographic module corresponds to the module's security policy and functional specification.
- Guidance Documents – concerned with the correct configuration, maintenance, administration and secure use of a cryptographic module.

3.3.10.1. Configuration Management

The specific security requirements for this subsection are:

(Levels 1, 2, 3, and 4) "A configuration management system shall be implemented for a cryptographic module and module components within the cryptographic boundary, and for associated module documentation. Each version of each configuration item (e.g., cryptographic module, module components, user guidance, security policy, and operating system) that comprises the module and associated documentation shall be assigned and labeled with a unique identification number."

3.3.10.2. Delivery and Operation

The specific security requirements for this subsection are:

(Security Levels 1, 2, 3, and 4) "Documentation shall specify the procedures for secure installation, initialization, and startup of a cryptographic module."

(Security Levels 2, 3, and 4) "In addition to the requirements of Security Level 1, documentation shall specify the procedures required for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators."

3.3.10.3. Development

This subsection subsumes the security requirements for *Software Security* as specified in FIPS 140-1. In FIPS 140-2, these requirements are extended to include the documentation of hardware design and to strengthen the requirements for documentation of software and firmware.

The requirements for documentation of software have been broadened to include firmware and hardware. More specifically, the FIPS 140-1 requirements:

> (Levels 1, 2, 3, and 4) "Documentation shall include a detailed explanation of the correspondence between the design of the software and the cryptographic security policy (i.e., the rules of operation)."
>
> (Levels 1, 2, 3, and 4) "Documentation shall include a complete source code listing for all software contained within the module. For each software module, software function and software procedures, the source code listing shall be annotated with comments that clearly depict the relationship of these software entities to the design of the software."

have been replaced in FIPS 140-2 by the requirements:

> (Levels 1, 2, 3, and 4) "Documentation shall specify the correspondence between the design of the hardware, software, and firmware components of a cryptographic module and the cryptographic module security policy (see Section 4.1)."
>
> (Levels 1, 2, 3, and 4) "If a cryptographic module contains software or firmware components, documentation shall specify the source code for the software and firmware components, annotated with comments that clearly depict the correspondence of the components to the design of the module."
>
> (Levels 1, 2, 3, and 4) "If a cryptographic module contains hardware components, documentation shall specify the schematics and/or Hardware Description Language (HDL) listings for the hardware components."

At Security Level 2, FIPS 140-2 has new requirements for functional specification of the interfaces and ports and the behavior of the cryptographic module:

> (Levels 2, 3 and 4) "Documentation shall specify a functional specification that informally describes a cryptographic module, the external ports and the interfaces of the module, and the purpose of the interfaces."

At Security Level 3, the use of high-level languages in the design has been extended to include firmware and hardware. Specifically, the FIPS 140-1 requirement:

> (Levels 3 and 4) "All software within a cryptographic module shall be implemented using a high-level language, except that the limited use of low-level languages (e.g., assembly languages) is allowed when it is essential to the performance of the module or when a high-level language is not available."

has been replaced by the FIPS 140-2 requirements:

> (Levels 3 and 4) "All software and firmware components within a cryptographic module shall be implemented using a high-level language, except that the limited use of a low-level language (e.g., assembly language or microcode) is allowed if essential to the performance

of the module or when a high-level language is not available."

(Levels 3 and 4) "If HDL is used, all hardware components within a cryptographic module shall be implemented using a high-level specification language."

At Security Level 4, FIPS 140-2 adds the new requirement:

(Level 4) "Documentation shall specify a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module security policy."

and modifies other documentation requirements:

"Documentation shall specify an informal proof of the correspondence between the formal model and the functional specification.

Documentation shall specify an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and postcondition annotations) and the functional specification."

3.3.10.4. Guidance Documents

The specific requirements for this subsection are:

(Levels 1, 2, 3, and 4) "Crypto officer guidance shall specify:

- the administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the crypto officer,
- procedures on how to administer the cryptographic module in a secure manner, and
- assumptions regarding user behavior that are relevant to the secure operation of the cryptographic module."

(Levels 1, 2, 3, and 4) "User guidance shall specify:

- the Approved security functions, physical ports, and logical interfaces available to the users of a cryptographic module, and
- all user responsibilities necessary for the secure operation of a cryptographic module."

3.3.11. Mitigation of Other Attacks

Certain types of cryptographic modules may be susceptible to attacks for which testable security requirements were not available at the time FIPS 140-2 was issued (e.g., power analysis, timing analysis, and fault induction) or are outside of the scope of the standard (e.g., TEMPEST). FIPS 140-2 requires the vendor to describe any such capabilities of the cryptographic modules:

(Levels 1, 2, 3, and 4) "If a cryptographic module is designed to mitigate one or more specific attacks, then the module's security policy shall specify the security mechanisms employed by the module to mitigate the attack(s). The existence and proper functioning of the security mechanisms will be validated when requirements and associated tests are developed."

4. DIFFERENCES IN APPENDIXES

This section details the differences in the Appendixes between FIPS 140-1 and 140-2.

Appendix A: Summary of Documentation Requirements

In FIPS 140-2, the information in Appendix A has been updated, commensurate with the changes to Section 4 of the standard.

Appendix B: Recommended Software Development Practices

In Appendix B of FIPS 140-2 the recommendations for modular design, programming, and documentation have been updated, consistent with modern practices.

Appendix C: Cryptographic Security Policy

In FIPS 140-2, Appendix C specifies detailed requirements for a *Security Policy* (not specified in FIPS 140-1) that must be provided by the vendor of the cryptographic module:

> "A cryptographic module security policy shall consist of a specification of the security rules, under which a module shall operate, including the security rules derived from the requirements of this standard and the additional security rules imposed by the vendor.
>
> The specification shall be sufficiently detailed to answer the following questions:
>
> - What access does operator *X*, performing service *Y* while in role *Z*, have to security-relevant data item *W* for every role, service, and security-related data item in the cryptographic module?
> - What physical security mechanisms are implemented to protect a cryptographic module and what actions are required to ensure that physical security of a module is maintained?
> - What security mechanisms are implemented in a cryptographic module to mitigate against attacks for which testable requirements are not defined in the Standard?
>
> A cryptographic security policy shall be expressed in terms of roles, services, and cryptographic keys and CSPs. At a minimum, the following shall be specified:
>
> - an identification and authentication (I&A) policy,
> - an access control policy,
> - a physical security policy, and
> - a security policy for mitigation of other attacks."

Further details are provided (in Appendix C of FIPS 140-2) as to what constitutes an acceptable specification of these components. Check lists are provided that serve as guides in determining whether or not the security policy is complete and contains the appropriate details.

Appendix D: Selected Bibliography

In FIPS 140-2, the citation of documents related to or supporting the Standard has been updated. Outdated references have been eliminated.

5. ANNEXES TO THE STANDARD

The lists of Approved security functions, protection profiles, random number generators, and key establishment techniques are expected to grow over time. In order to dynamically incorporate these changes in the requirements, these lists will be maintained in the following Annexes to FIPS 140-2:

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: csrc.nist.gov/cryptval.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Recommended Protection Profiles*, available at URL: csrc.nist.gov/cryptval.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: csrc.nist.gov/cryptval.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: csrc.nist.gov/cryptval.